Foundation of Cryptography (0368-4162-01), Lecture 7

Encryption Schemes

Iftach Haitner, Tel Aviv University

January 3, 2012

Section 1

Definition

Definition

Definition 1 (encryption scheme)

A trippet of PPT's $(G, \mathsf{E}, \mathsf{D})$ such that

1. $G(1^n)$ outputs a key $(e, d) \in \{0,1\}^*$
2. $\mathsf{E}(e, m)$ outputs an encryption c
3. $\mathsf{D}(d, c)$ outputs a message

Correctness: $\mathsf{D}(d, \mathsf{E}(e, m)) = m$, for any $(e, d) \in \mathrm{Supp}(G(1^n))$ and $m \in \{0,1\}^*$

Definition

Definition 1 (encryption scheme)

A trippet of PPT's $(G, \mathrm{E}, \mathrm{D})$ such that

1. $G(1^n)$ outputs a key $(e, d) \in \{0,1\}^*$
2. $\mathrm{E}(e, m)$ outputs an encryption c
3. $\mathrm{D}(d, c)$ outputs a message

Correctness: $\mathrm{D}(d, \mathrm{E}(e, m)) = m$, for any $(e, d) \in \mathrm{Supp}(G(1^n))$ and $m \in \{0,1\}^*$

- e – encryption key, d – decryption key
- m – plaintext, $c =, \mathrm{E}(e, m)$ – ciphertext
- $E_e(m) \equiv E(e, m)$ and $D_d(c) \equiv D(d, c)$,

Definition

Definition 1 (encryption scheme)

A trippet of PPT's $(G, \mathrm{E}, \mathrm{D})$ such that

1. $G(1^n)$ outputs a key $(e, d) \in \{0,1\}^*$
2. $\mathrm{E}(e, m)$ outputs an encryption c
3. $\mathrm{D}(d, c)$ outputs a message

Correctness: $\mathrm{D}(d, \mathrm{E}(e, m)) = m$, for any $(e, d) \in \mathrm{Supp}(G(1^n))$ and $m \in \{0,1\}^*$

- e – encryption key, d – decryption key
- m – plaintext, $c =, \mathrm{E}(e, m)$ – ciphertext
- $E_e(m) \equiv E(e, m)$ and $D_d(c) \equiv D(d, c)$,
- public/private key

Definition

Definition 1 (encryption scheme)

A trippet of PPT's $(G, \mathrm{E}, \mathrm{D})$ such that

1. $G(1^n)$ outputs a key $(e, d) \in \{0,1\}^*$
2. $\mathrm{E}(e, m)$ outputs an encryption c
3. $\mathrm{D}(d, c)$ outputs a message

Correctness: $\mathrm{D}(d, \mathrm{E}(e, m)) = m$, for any $(e, d) \in \mathrm{Supp}(G(1^n))$ and $m \in \{0,1\}^*$

- e – encryption key, d – decryption key
- m – plaintext, $c =, \mathrm{E}(e, m)$ – ciphertext
- $E_e(m) \equiv E(e, m)$ and $D_d(c) \equiv D(d, c)$,

- public/private key
- negligible error

Definition

Definition 1 (encryption scheme)

A trippet of PPT's $(G, \mathrm{E}, \mathrm{D})$ such that

1. $G(1^n)$ outputs a key $(e, d) \in \{0,1\}^*$
2. $\mathrm{E}(e, m)$ outputs an encryption c
3. $\mathrm{D}(d, c)$ outputs a message

Correctness: $\mathrm{D}(d, \mathrm{E}(e, m)) = m$, for any $(e, d) \in \mathrm{Supp}(G(1^n))$ and $m \in \{0,1\}^*$

- e – encryption key, d – decryption key
- m – plaintext, $c =, \mathrm{E}(e, m)$ – ciphertext
- $E_e(m) \equiv E(e, m)$ and $D_d(c) \equiv D(d, c)$,

- public/private key
- negligible error

Security

- What would we like to achieve?

Security

- What would we like to achieve?
- Dream version: exits $\ell \in$ poly such that for any $n \in \mathbb{N}$ and $x \in \{0,1\}^*$:

$$(E_{G(1^n)_1}(x)) \equiv U_{\ell(n)}$$

Security

- What would we like to achieve?
- Dream version: exits $\ell \in$ poly such that for any $n \in \mathbb{N}$ and $x \in \{0,1\}^*$:

$$(E_{G(1^n)_1}(x)) \equiv U_{\ell(n)}$$

Shannon – only for x with $|x| \leq |G(1^n)_1|$

Semantic Security

1. Ciphertext reveal “no information" about the plaintext

Semantic Security

1. Ciphertext reveal “no information" about the plaintext
2. Formulate via the simulation paradigm

Semantic Security

1. Ciphertext reveal “no information" about the plaintext
2. Formulate via the simulation paradigm
3. Cannot hide the message length

Semantic security – private-key model

Definition 2 (Semantic Security – private-key model)

An encryption scheme $(G, \mathsf{E}, \mathsf{D})$ is semantically secure in the private-key model, if for any PPT A, $\exists$ PPT A' s.t. for any polynomially-bounded ensemble $\mathcal{X} = \{\mathcal{X}_n\}_{n \in \mathbb{N}}$ and every polynomially-bounded functions $h, f \colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\Big| \Pr_{x \leftarrow \mathcal{X}_n, e \leftarrow G(1^n)_1} [\mathsf{A}(1^n, E_e(x), 1^{|x|}, h(1^n, x)) = f(1^n, x)] \\ - \Pr_{x \leftarrow \mathcal{X}_n} [\mathsf{A}'(1^n, h(1^n, x)) = f(1^n, x)] \Big| = \operatorname{neg}(n)$$

Semantic security – private-key model

Definition 2 (Semantic Security – private-key model)

An encryption scheme $(G, \mathsf{E}, \mathsf{D})$ is semantically secure in the private-key model, if for any PPT A, $\exists$ PPT A' s.t. for any polynomially-bounded ensemble $\mathcal{X} = \{\mathcal{X}_n\}_{n \in \mathbb{N}}$ and every polynomially-bounded functions $h, f \colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\Big| \Pr_{x \leftarrow \mathcal{X}_n, e \leftarrow G(1^n)_1}[\mathsf{A}(1^n, E_e(x), 1^{|x|}, h(1^n, x)) = f(1^n, x)] \\ - \Pr_{x \leftarrow \mathcal{X}_n}[\mathsf{A}'(1^n, h(1^n, x)) = f(1^n, x)] \Big| = \operatorname{neg}(n)$$

- polynomially-bounded?

Semantic security – private-key model

Definition 2 (Semantic Security – private-key model)

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ is semantically secure in the private-key model, if for any PPT A, $\exists$ PPT A$'$ s.t. for any polynomially-bounded ensemble $\mathcal{X} = \{\mathcal{X}_n\}_{n\in\mathbb{N}}$ and every polynomially-bounded functions $h, f \colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\Big|\Pr_{x\leftarrow\mathcal{X}_n, e\leftarrow G(1^n)_1}[\mathrm{A}(1^n, E_e(x), 1^{|x|}, h(1^n, x)) = f(1^n, x)] \\ -\Pr_{x\leftarrow\mathcal{X}_n}[\mathrm{A}'(1^n, h(1^n, x)) = f(1^n, x)]\Big| = \mathrm{neg}(n)$$

- polynomially-bounded? for simplicity we assume polynomial length

Semantic security – private-key model

Definition 2 (Semantic Security – private-key model)

An encryption scheme $(G, \mathsf{E}, \mathsf{D})$ is semantically secure in the private-key model, if for any PPT A, $\exists$ PPT A$'$ s.t. for any polynomially-bounded ensemble $\mathcal{X} = \{\mathcal{X}_n\}_{n\in\mathbb{N}}$ and every polynomially-bounded functions $h, f \colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\Big|\Pr_{x\leftarrow\mathcal{X}_n, e\leftarrow G(1^n)_1}[\mathsf{A}(1^n, E_e(x), 1^{|x|}, h(1^n, x)) = f(1^n, x)] \\ -\Pr_{x\leftarrow\mathcal{X}_n}[\mathsf{A}'(1^n, h(1^n, x)) = f(1^n, x)]\Big| = \operatorname{neg}(n)$$

- polynomially-bounded? for simplicity we assume polynomial length
- 1^n and $1^{|x|}$ are not really needed

Semantic security – private-key model

Definition 2 (Semantic Security – private-key model)

An encryption scheme $(G, \mathsf{E}, \mathsf{D})$ is semantically secure in the private-key model, if for any PPT A, $\exists$ PPT A' s.t. for any polynomially-bounded ensemble $\mathcal{X} = \{\mathcal{X}_n\}_{n \in \mathbb{N}}$ and every polynomially-bounded functions $h, f \colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\Big| \Pr_{x \leftarrow \mathcal{X}_n, e \leftarrow G(1^n)_1}[\mathsf{A}(1^n, E_e(x), 1^{|x|}, h(1^n, x)) = f(1^n, x)] \\ - \Pr_{x \leftarrow \mathcal{X}_n}[\mathsf{A}'(1^n, h(1^n, x)) = f(1^n, x)] \Big| = \operatorname{neg}(n)$$

- polynomially-bounded? for simplicity we assume polynomial length
- 1^n and $1^{|x|}$ are not really needed
- Non-uniform definition

Semantic security – private-key model

Definition 2 (Semantic Security – private-key model)

An encryption scheme $(G, \mathsf{E}, \mathsf{D})$ is semantically secure in the private-key model, if for any PPT A, $\exists$ PPT A' s.t. for any polynomially-bounded ensemble $\mathcal{X} = \{\mathcal{X}_n\}_{n\in\mathbb{N}}$ and every polynomially-bounded functions $h, f\colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\Big|\Pr_{x\leftarrow\mathcal{X}_n, e\leftarrow G(1^n)_1}[\mathsf{A}(1^n, E_e(x), 1^{|x|}, h(1^n, x)) = f(1^n, x)] \\ -\Pr_{x\leftarrow\mathcal{X}_n}[\mathsf{A}'(1^n, h(1^n, x)) = f(1^n, x)]\Big| = \operatorname{neg}(n)$$

- polynomially-bounded? for simplicity we assume polynomial length
- 1^n and $1^{|x|}$ are not really needed
- Non-uniform definition
- Relation to $\mathcal{ZK}$

Semantic security – public-key model

Definition 3 (Semantic Security – public-key model)

An encryption scheme $(G, \mathsf{E}, \mathsf{D})$ is semantically secure in the public-key model, if for any PPT A, $\exists$ PPT A' s.t. for any polynomially-bounded ensemble $\mathcal{X} = \{\mathcal{X}_n\}_{n\in\mathbb{N}}$ and every polynomially-bounded functions $h, f\colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\Big|\Pr_{x\leftarrow\mathcal{X}_n,(e,d)\leftarrow G(1^n)}[\mathsf{A}(1^n, e, E_e(x), 1^{|x|}, h(1^n, x)) = f(1^n, x)] \\ -\Pr_{x\leftarrow\mathcal{X}_n}[\mathsf{A}'(1^n, 1^{|x|}, h(1^n, x)) = f(1^n, x)]\Big| = \operatorname{neg}(n)$$

Indistinguishablity of encryptions

- The encryption of two strings is indistinguishable

Indistinguishablity of encryptions

- The encryption of two strings is indistinguishable
- Less intuitive than semantic security, but easier to work with

Indistinguishablity of encryptions – private-key model

Definition 4 (Indistinguishablity of encryptions – private-key model)

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ has indistinguishable encryptions in the private-key model, if for any p, ℓ poly(n), $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ and polynomial-time B,

$$\Big|\Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(x_n)) = 1] \\ -\Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(y_n)) = 1]\Big| = \mathrm{neg}(n)$$

Indistinguishablity of encryptions – private-key model

Definition 4 (Indistinguishablity of encryptions – private-key model)

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ has indistinguishable encryptions in the private-key model, if for any p, ℓ poly(n), $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ and polynomial-time B,

$$\left|\Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(x_n)) = 1] \right.$$
$$\left. -\Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(y_n)) = 1]\right| = \mathrm{neg}(n)$$

- Non-uniform definition

Indistinguishablity of encryptions – private-key model

Definition 4 (Indistinguishablity of encryptions – private-key model)

An encryption scheme $(G, \mathsf{E}, \mathsf{D})$ has indistinguishable encryptions in the private-key model, if for any p, ℓ poly(n), $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ and polynomial-time B,

$$\left|\Pr_{e\leftarrow G(1^n)_1}[\mathsf{B}(z_n, E_e(x_n)) = 1] - \Pr_{e\leftarrow G(1^n)_1}[\mathsf{B}(z_n, E_e(y_n)) = 1]\right| = \mathrm{neg}(n)$$

- Non-uniform definition
- Public-key model

Equivalence of definitions

Theorem 5

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ *is semantically secure iff is has indistinguishable encryptions.*

Equivalence of definitions

Theorem 5

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ *is semantically secure iff is has indistinguishable encryptions.*

We prove the private key case

Indistinguishablity $\Longrightarrow$ Semantic Security

Indistinguishablity $\implies$ Semantic Security

Fix $\mathcal{X}$, A, f and h, be as in Definition 2.

Indistinguishablity $\Longrightarrow$ Semantic Security

Fix $\mathcal{X}$, A, f and h, be as in Definition 2. We construct A′ as

Algorithm 6 (A′)

Input: 1^n, $1^{|x|}$ and $h(x)$

1. $e \leftarrow G(1^n)_1$
2. $c = E_e(1^{|x|})$
3. Output $\mathrm{A}(1^n, c, 1^{|x|}, h(x))$

Indistinguishablity $\implies$ Semantic Security

Fix $\mathcal{X}$, A, f and h, be as in Definition 2. We construct A′ as

Algorithm 6 (A′)

Input: 1^n, $1^{|x|}$ and $h(x)$

1. $e \leftarrow G(1^n)_1$
2. $c = E_e(1^{|x|})$
3. Output A$(1^n, c, 1^{|x|}, h(x))$

Claim 7

A′ is a good simulator for A (according to Definition 2)

Proving Claim 7

Assume exists infinite $\mathcal{I} \subseteq \mathbb{N}$ and $p \in$ poly s.t. for any $n \in \mathcal{I}$:

$$\begin{aligned} \Big| \Pr_{x \leftarrow \mathcal{X}_n, e \leftarrow G(1^n)_1}[\mathsf{A}(1^n, E_e(x), h(1^n, x)) = f(1^n, x)] \\ - \Pr_{x \leftarrow \mathcal{X}_n}[\mathsf{A}'(1^n, h(1^n, x)) = f(1^n, x)] \Big| > 1/p(n) \end{aligned} \tag{1}$$

Proving Claim 7

Assume exists infinite $\mathcal{I} \subseteq \mathbb{N}$ and $p \in$ poly s.t. for any $n \in \mathcal{I}$:

$$\begin{aligned} \Big| \Pr_{x \leftarrow \mathcal{X}_n, e \leftarrow G(1^n)_1}[\mathsf{A}(1^n, E_e(x), h(1^n, x)) = f(1^n, x)] \\ - \Pr_{x \leftarrow \mathcal{X}_n}[\mathsf{A}'(1^n, h(1^n, x)) = f(1^n, x)] \Big| > 1/p(n) \end{aligned} \tag{1}$$

Fix $n \in \mathcal{I}$ and let $x \in \mathrm{Supp}(\mathcal{X}_n)$ be a value that maximize Equation (1). We construct B and contradicts the indistinguishability of the scheme with respect to $\{(x_n = x, y_n = 1^{|x|})\}$ and $\{z_n = (h(1^n, x), f(1^n, x))\}$.

Algorithm 8 (B)

Input: 1^n, $z_n = (h(1^n, x), f(1^n, x))$, c
Output 1 iff $\mathsf{A}(1^n, c, 1^{|x|}, h(x)) = f(1^n, x)$

Semantic Security $\implies$ Indistinguishablity

Assume $\exists$ B, $\{(x_n, y_n)\}_{n\in\mathbb{N}}$ and $\{z_n\}_{n\in\mathbb{N}}$ that contradict the semantic security of semantic security.

Semantic Security $\Longrightarrow$ Indistinguishablity

Assume $\exists$ B, $\{(x_n, y_n)\}_{n\in\mathbb{N}}$ and $\{z_n\}_{n\in\mathbb{N}}$ that contradict the semantic security of semantic security.
Let $\mathcal{X}_n$ be x_n wp $\frac{1}{2}$ and y_n otherwise, let $f(1^n, x_n) = 1$ and $f(1^n, y_n) = 0$ and let $h(1^n, \cdot = z_n)$. Finally, A$(1^n, \cdot, c, z_n)$ returns B(z_n, c).

Security Under Multiple Encryptions

Security Under Multiple Encryptions

Definition 9 (Indistinguishablity for multiple encryptions – private-key model)

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ has indistinguishable encryptions for multiple messages in the private-key model, if for any p, ℓ, t poly(n), $\{x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n \in \mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n \in \mathbb{N}}$ and polynomial-time B,

$$\Big| \Pr_{e \leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(x_{n,1}), \ldots E_e(x_{n,t(n)})) = 1] - \Pr_{e \leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(y_{n,1}), \ldots E_e(y_{n,t(n)})) = 1 \Big| = \mathrm{neg}(n)$$

Security Under Multiple Encryptions

Definition 9 (Indistinguishablity for multiple encryptions – private-key model)

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ has indistinguishable encryptions for multiple messages in the private-key model, if for any p, ℓ, t poly(n),
$\{x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n \in \mathbb{N}}$,
$\{z_n \in \{0,1\}^{p(n)}\}_{n \in \mathbb{N}}$ and polynomial-time B,

$$\Big|\Pr_{e \leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(x_{n,1}), \ldots E_e(x_{n,t(n)})) = 1]$$
$$-\Pr_{e \leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(y_{n,1}), \ldots E_e(y_{n,t(n)})) = 1\Big| = \mathrm{neg}(n)$$

- Different length messages

Security Under Multiple Encryptions

Definition 9 (Indistinguishablity for multiple encryptions – private-key model)

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ has indistinguishable encryptions for multiple messages in the private-key model, if for any p, ℓ, t poly(n), $\{x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ and polynomial-time B,

$$\Big|\Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(x_{n,1}), \ldots E_e(x_{n,t(n)})) = 1] - \Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(y_{n,1}), \ldots E_e(y_{n,t(n)})) = 1\Big| = \mathrm{neg}(n)$$

- Different length messages
- Semantic security version

Security Under Multiple Encryptions

Definition 9 (Indistinguishablity for multiple encryptions – private-key model)

An encryption scheme $(G, \mathrm{E}, \mathrm{D})$ has indistinguishable encryptions for multiple messages in the private-key model, if for any p, ℓ, t poly(n), $\{x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ and polynomial-time B,

$$\left|\Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(x_{n,1}), \ldots E_e(x_{n,t(n)})) = 1] - \Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(y_{n,1}), \ldots E_e(y_{n,t(n)})) = 1\right| = \mathrm{neg}(n)$$

- Different length messages
- Semantic security version
- Public-key definition

Multiple Encryption in the Public-Key Model

Theorem 10

A public-key encryption scheme has indistinguishable encryptions for multiple messages, iff it has indistinguishable encryptions for a single message.

Proof: Assume $(G, \mathrm{E}, \mathrm{D})$ is public-key secure for a single message and not for multiple messages with respect to B, $\{x_{1,t(n)}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$.

Multiple Encryption in the Public-Key Model

Theorem 10

A public-key encryption scheme has indistinguishable encryptions for multiple messages, iff it has indistinguishable encryptions for a single message.

Proof: Assume $(G, \mathrm{E}, \mathrm{D})$ is public-key secure for a single message and not for multiple messages with respect to B,
$\{x_{1,t(n)}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$,
$\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$.
It follows that for some function $i(n) \in [t(n)]$

$$\begin{aligned}&\Big|\Pr[\mathrm{B}(1^n, e, E_e(x_{n,1}), \ldots, E_e(x_{n,i-1}), E_e(y_{n,i}) \ldots, E_e(y_{n,t(n)})) = 1]\\ -&\Pr[\mathrm{B}(1^n, e, E_e(x_{n,1}), \ldots, E_e(x_{n,i}), E_e(y_{n,i+1}) \ldots, E_e(y_{n,t(n)})) = 1]\Big|\\ &> \mathrm{neg}(n)\end{aligned}$$

where in both cases $e \leftarrow G(1^n)_1$

Algorithm 11 (B′)

Input: 1^n, $z_n = i(n)$, e ,c
Return $\mathrm{B}(c, E_e(x_{n,1}), \ldots, E_e(x_{n,i-1}), c, E_e(y_{n,i+1}) \ldots, E_e(y_{n,t(n)}))$

Algorithm 11 (B′)

Input: 1^n, $z_n = i(n)$, e ,c
Return $\mathrm{B}(c, E_e(x_{n,1}), \ldots, E_e(x_{n,i-1}), c, E_e(y_{n,i+1}) \ldots, E_e(y_{n,t(n)}))$

B′ is critically using the public key

Multiple Encryption in the Private-Key Model

Fact 12

Assume (non uniform) OWFs exists, there exists an encryption scheme that has private-key indistinguishable encryptions for a single messages, bit not for multiple messages

Multiple Encryption in the Private-Key Model

Fact 12

Assume (non uniform) OWFs exists, there exists an encryption scheme that has private-key indistinguishable encryptions for a single messages, bit not for multiple messages

Proof: Let $g\colon \{0,1\}^n \mapsto \{0,1\}^{n+1}$ be a (non-uniform) PRG, and for $i \in \mathbb{N}$ let g_i be its "iterated extension" to output of length i (see Lecture 2.).

Construction 13

- $G(1^n)$ outputs $e \leftarrow \{0,1\}^n$,
- $\mathsf{E}_e(m)$ outputs $g_{|m|}(e) \oplus m$
- $\mathsf{D}_e(c)$ outputs $g_{|c|}(e) \oplus c$

Claim 14

$(G, \mathrm{E}, \mathrm{D})$ has a indistinguishable encryptions for a single message

Proof:

Claim 14

$(G, \mathrm{E}, \mathrm{D})$ has a indistinguishable encryptions for a single message

Proof: Assume not, and let B, $\{x_n, y_n\}_{n\in\mathbb{N}}$ and $\{z_n\}_{n\in\mathbb{N}}$ be the triplet that realizes it.

Claim 14

$(G, \mathrm{E}, \mathrm{D})$ has a indistinguishable encryptions for a single message

Proof: Assume not, and let B, $\{x_n, y_n\}_{n \in \mathbb{N}}$ and $\{z_n\}_{n \in \mathbb{N}}$ be the triplet that realizes it.
Wlog,

$$\left|\Pr[\mathrm{B}(z_n, g_{|x_n|}(U_n) \oplus x_n) = 1] - \Pr[\mathrm{B}(z_n, U_{|x_n|} \oplus x_n) = 1]\right| > \mathrm{neg}(n) \tag{2}$$

Claim 14

$(G, \mathsf{E}, \mathsf{D})$ has a indistinguishable encryptions for a single message

Proof: Assume not, and let B, $\{x_n, y_n\}_{n \in \mathbb{N}}$ and $\{z_n\}_{n \in \mathbb{N}}$ be the triplet that realizes it.
Wlog,

$$\left|\Pr[\mathsf{B}(z_n, g_{|x_n|}(U_n) \oplus x_n) = 1] - \Pr[\mathsf{B}(z_n, U_{|x_n|} \oplus x_n) = 1]\right| > \operatorname{neg}(n) \tag{2}$$

Hence, B implies a (non -uniform) distinguisher for g

Claim 14

$(G, \mathrm{E}, \mathrm{D})$ has a indistinguishable encryptions for a single message

Proof: Assume not, and let B, $\{x_n, y_n\}_{n\in\mathbb{N}}$ and $\{z_n\}_{n\in\mathbb{N}}$ be the triplet that realizes it.
Wlog,

$$\left|\Pr[\mathrm{B}(z_n, g_{|x_n|}(U_n) \oplus x_n) = 1] - \Pr[\mathrm{B}(z_n, U_{|x_n|} \oplus x_n) = 1]\right| > \mathrm{neg}(n) \tag{2}$$

Hence, B implies a (non -uniform) distinguisher for g

Claim 15

$(G, \mathrm{E}, \mathrm{D})$ does not have a indistinguishable encryptions for multiple messages

Claim 14

$(G, \mathsf{E}, \mathsf{D})$ has a indistinguishable encryptions for a single message

Proof: Assume not, and let B, $\{x_n, y_n\}_{n\in\mathbb{N}}$ and $\{z_n\}_{n\in\mathbb{N}}$ be the triplet that realizes it.
Wlog,

$$\left|\Pr[\mathsf{B}(z_n, g_{|x_n|}(U_n) \oplus x_n) = 1] - \Pr[\mathsf{B}(z_n, U_{|x_n|} \oplus x_n) = 1]\right| > \operatorname{neg}(n) \quad (2)$$

Hence, B implies a (non -uniform) distinguisher for g

Claim 15

$(G, \mathsf{E}, \mathsf{D})$ does not have a indistinguishable encryptions for multiple messages

Proof:

Claim 14

$(G, \mathrm{E}, \mathrm{D})$ has a indistinguishable encryptions for a single message

Proof: Assume not, and let B, $\{x_n, y_n\}_{n\in\mathbb{N}}$ and $\{z_n\}_{n\in\mathbb{N}}$ be the triplet that realizes it.
Wlog,

$$\left|\Pr[\mathrm{B}(z_n, g_{|x_n|}(U_n) \oplus x_n) = 1] - \Pr[\mathrm{B}(z_n, U_{|x_n|} \oplus x_n) = 1]\right| > \mathrm{neg}(n) \tag{2}$$

Hence, B implies a (non -uniform) distinguisher for g

Claim 15

$(G, \mathrm{E}, \mathrm{D})$ does not have a indistinguishable encryptions for multiple messages

Proof: Take $x_{n,1} = x_{n,2}$ and $y_{n,1} \neq x_{n,2}$ and $\mathrm{D}(c_1, c_2)$ outputs 1 iff $c_1 = c_2$

Section 2

Constructions

Private key indistinguishable encryptions for multiple messages

Construction 16

- $G(1^n)$ outputs $e \leftarrow \{0,1\}^n$,
- $\mathrm{E}_e(m)$ outputs $g_{|m|}(e) \oplus m$
- $\mathrm{D}_e(c)$ outputs $g_{|c|}(e) \oplus c$